Complete Proof Systems for First Order Interval Temporal Logic

Bruno Dutertre
Department of Computer Science
Royal Holloway, University of London
Egham, Surrey TW20 0EX, United Kingdom

Abstract

Different interval modal logics have been proposed for reasoning about the temporal behaviour of digital systems. Some of them are purely propositional and only enable the specification of qualitative time requirements. Others, such as ITL and the duration calculus, are first order logics which support the expression of quantitative, real-time requirements. These two logics have in common the presence of a binary modal operator 'chop' interpreted as the action of splitting an interval into two parts.

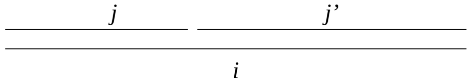
Proof systems for ITL or the duration calculus have been proposed but little is known about their power. This paper present completeness results for a variant of ITL where 'chop' is the only modal operator. We consider several classes of models for ITL which make different assumptions about time and we construct a complete and sound proof system for each class.

1 Introduction

Digital systems are increasingly used in applications where they interact with physical processes. In these applications, systems often have to meet real-time constraints: they have to react to events within a prescribed time interval, to produce output before a certain delay has elapsed, etc. In order to reason about such real-time applications, quantitative as well as qualitative time requirements have to be considered. For this purpose, various real-time temporal logics have been proposed.

For example, several real-time extensions of linear propositional temporal logic (PTL) are reviewed and compared in [3]. Although these logics are substantially more complex than ordinary PTL, some of them conserve interesting properties such as decidability [3]. Similarly, real-time extensions of the branching time logic CTL have been introduced [8] for which model checking is decidable [2, 12].

In the above logics, formulas are interpreted over states which represent instantaneous situations; time points are the basic entities. Other formalisms adopt a different semantics and interpret formulas over intervals of time [14, 10, 20]. Among such interval modal logics, ITL [14] and more specifically the duration calculus [6, 17] have been proposed for reasoning about real-time systems. These two formalisms are first order logics which incorporate a binary modal operator (denoted by ;) interpreted as the operation of 'chopping' an interval into two parts: a formula $(f; g)$ is satisfied by an interval i if i can be split into two sub-intervals j and j' as follows



with j satisfying f and j' satisfying g.

Different deductive systems exist for both ITL [15] and the duration calculus [11, 19] but little is known about their power. However, close links between the two logics have been established in [11]: a complete proof system for a dense-timed ITL would yield a complete deductive system for the duration calculus. In the propositional case, complete axiomatizations have been proposed for modal logics which contain the chop operator [18, 16, 20]. Some of these logics are known to be decidable [18]. Except for restricted fragments, the duration calculus (and ITL) are not decidable [5].

This paper presents completeness results for first order ITL, in a variant similar to the one used in [11] which contains no other modal operator than chop[1]. We consider several classes of models and we show how a complete and sound proof system can be constructed for each class.

First, we give a *possible worlds* semantics for ITL. We define an axiomatic system S adequate for a general class $\mathcal{C}$ of models. The main interest of this result is to provide a model construction technique which can be applied to any extension of S.

[1]Other modalities such as $\Box$ (in all sub-intervals) or $\Diamond$ (in some sub-interval) can still be easily defined in terms of chop (see [11] for example).

In a second part, we concentrate on *interval models* similar to the traditional ITL models presented in [11, 15]. By making various assumptions about time and about the operations available for expressing real-time constraints, one can define several classes of interval models. Provided the assumptions can be expressed in ordinary first order logic, a complete and sound ITL deductive system can be devised for any such class of models.

2 First order ITL

2.1 Syntax

A language for first order ITL with equality consists of a denumerable collection of predicate and function symbols. With each symbol is associated an arity; predicate symbols of arity 0 are propositions and function symbols of arity 0 are constants.

In addition, we distinguish between flexible and rigid symbols (we use the terminology of [1, 9]). Rigid symbols are intended to represent fixed entities, their interpretation will be the same in all worlds or intervals. On the contrary, flexible symbols represent entities which may vary for different intervals. The language includes at least one flexible constant ℓ that represents the length of intervals.

The vocabulary also includes variables, propositional connectives, the existential quantifier, the symbol '=', and a single modal operator ';' called chop. The equality symbol is considered as a supplementary rigid predicate symbol of arity 2.

Terms and atomic formulas are defined as in first order logic with equality. The formation rules are the following:

- any variable x and any constant a is a term,
- if $t_1, \ldots, t_n$ are terms and α is a function symbol of arity $n > 0$ then $\alpha(t_1, \ldots, t_n)$ is a term,
- any proposition p is an atomic formula,
- if $t_1, \ldots, t_n$ are terms and ϕ is a predicate symbol of arity $n > 0$ then $\phi(t_1, \ldots, t_n)$ is an atomic formula.

Finally, formulas are obtained by the rules:

- any atomic formula is a formula,
- if f_1 and f_2 are formulas then $(f_1 \wedge f_2)$, $(\neg f_1)$, $(f_1 ; f_2)$ are formulas,
- if f is a formula and x a variable then $(\exists x) f$ is a formula.

The other usual connectives $\vee$, $\Rightarrow$, and $\Leftrightarrow$, as well as the universal quantifier are introduced as abbreviations.

We say that a term or a formula is rigid if it does not contain any flexible symbol. In particular, variables are rigid. A formula is said to be chop-free if it does contain the chop connective.

2.2 Semantics

We adopt an approach similar to [20]. We give a Kripke-style *possible worlds* semantics for ITL and we consider the more traditional *interval semantics* as a special case. In this section we present a general notion of models and we introduce a refinement which imposes a constraint on the interpretation of the symbol ℓ. Interval models will be defined in section 4.

Definition 1 *A model for an ITL language $\mathcal{L}$ is a quadruple (W, R, D, I) where*

- *W is a non-empty set of possible worlds and R a ternary relation on W,*
- *D is a non-empty set,*
- *I is a function which assigns to each symbol s of $\mathcal{L}$ and each world w in W an interpretation $I(s, w)$ as follows:*
  - *if s is an n-ary function symbol, $I(s, w)$ is a function from D^n to D,*
  - *if s is an n-ary predicate symbol, $I(s, w)$ is an n-ary relation on D,*

  and such that the interpretation of rigid symbols is the same in all worlds.

The pair (W, R) is called the *frame* and the set D the *domain* of the model.

Given a model $\mathcal{M}$, a meaning is associated in each world of W to every term and formula. This depends on particular values assigned to variables. Under a valuation v (a mapping which assigns a value to each variable), $v, w \models f$ denotes that a formula f is satisfied in a world w. We also write $\mathcal{M}, w \models f$ when the model is not clear from the context. The valuation is irrelevant and not written when f is a closed formula.

The semantics is defined by induction on terms and formulas in a standard way, with R playing a role similar to the binary accessibility relation in ordinary modal logic [13]:

$$v, w \models (f ; g) \quad \text{iff} \quad \text{there are } w_1, w_2, \begin{cases} v, w_1 \models f \\ v, w_2 \models g \\ R(w_1, w_2, w). \end{cases}$$

We use a fixed-domain semantics; the domain D does not change with worlds. As a consequence, and since a valuation is fixed for all worlds, a variant of Barcan formula [13] holds: formulas of the form $((\exists x)f; g) \Rightarrow (\exists x)(f; g)$ and $(g; (\exists x)f) \Rightarrow (\exists x)(g; f)$ are valid, provided x is not free in g.

Since it is intended to represent the length of intervals, the flexible symbol ℓ plays an essential role in the logic. Various axioms will be introduced corresponding to "natural" properties of length. An important assumption is that two distinct prefixes or suffixes of an interval have different lengths. Although no precise notion of interval models has been given yet, we can extend this constraint to possible worlds:

Definition 2 *A model $\mathcal{M} = (W, R, D, I)$ for a language $\mathcal{L}$ is an S-model if for any worlds w, w_1, w_2, w_1', and w_2' of W such that $R(w_1, w_2, w)$ and $R(w_1', w_2', w)$,*

- *if $I(\ell, w_1) = I(\ell, w_1')$ then $w_2 = w_2'$,*
- *if $I(\ell, w_2) = I(\ell, w_2')$ then $w_1 = w_1'$.*

The definition implies a *single decomposition* property: if $R(w_1, w_2, w)$ then there is no world w_1' other than w_1 such that $R(w_1', w_2, w)$ and there is no w_2' other than w_2 such that $R(w_1, w_2', w)$.

3 A first proof system

3.1 The system S

We call S the deductive system which incorporates the following modal axioms:

$$\text{A1:}\quad \begin{array}{l} (f; g) \wedge \neg(f; h) \Rightarrow (f; g \wedge \neg h) \\ (f; g) \wedge \neg(h; g) \Rightarrow (f \wedge \neg h; g) \end{array}$$

$$\text{R:}\quad \begin{array}{ll} (f; g) \Rightarrow f & \text{if } f \text{ is a rigid formula} \\ (f; g) \Rightarrow g & \text{if } g \text{ is a rigid formula} \end{array}$$

$$\text{B:}\quad \begin{array}{ll} ((\exists x)f; g) \Rightarrow (\exists x)(f; g) & \text{if } x \text{ is not free in } g \\ (f; (\exists x)g) \Rightarrow (\exists x)(f; g) & \text{if } x \text{ is not free in } f \end{array}$$

$$\text{L1:}\quad \begin{array}{l} (\ell = x; f) \Rightarrow \neg(\ell = x; \neg f) \\ (f; \ell = x) \Rightarrow \neg(\neg f; \ell = x) \end{array}$$

and the following inference rules

$$\text{MP: } \frac{f \quad f \Rightarrow g}{g}, \qquad \text{G: } \frac{f}{(\forall x)f},$$

$$\text{N: } \frac{f}{\neg(\neg f; g)} \text{ and } \frac{f}{\neg(g; \neg f)},$$

$$\text{Mono: } \frac{f \Rightarrow g}{(f; h) \Rightarrow (g; h)} \text{ and } \frac{f \Rightarrow g}{(h; f) \Rightarrow (h; g)}.$$

MP and G are the usual rules of modus ponens and generalisation, N and Mono are the necessitation and monotonicity rules, respectively,

In addition, S contains first order and propositional axioms and the axioms of identity. These can be taken as in any complete system for first order logic except for some restrictions on the instantiation of quantified formulas. We can use the following axiom

$$\text{Q:}\quad f(t) \Rightarrow (\exists x)f(x),$$

with the constraint that t must be free for x in $f(x)$ and that, in addition, either $f(x)$ is chop-free or t is a rigid term. The latter restrictions prevent the substitution of a flexible term which may denote different entities in different contexts by a variable which represents a single, global object.

3.2 Soundness

It is easy to check that any instance of the three axioms A1, R and B is valid. R simply says that the truth or falsity of rigid formulas is the same in any world of a model and B is Barcan formula translated to ITL. Similarly, the inference rules all preserve validity.

Axiom L1 is not valid in general but it is in the class $\mathcal{C}$ of S-models. This follows immediately from definition 2. Globally, the axiomatic system S is then sound for the class $\mathcal{C}$: for any formula f, if $\vdash_S f$ then f is valid in $\mathcal{C}$. In the next section, we show that S is also complete for this class.

3.3 Completeness

Let $\mathcal{L}$ be an arbitrary ITL-language. We have to show that any sentence f of $\mathcal{L}$ such that $\neg f$ is not provable by S is satisfied by an S-model. In its broad lines, the construction follows [1, 9].

Consistent and maximal consistent sets of sentences are defined in a standard way [13]. A set Γ of sentences of $\mathcal{L}$ is *consistent* if there is no finite subset $\{f_1, \ldots, f_n\}$ of Γ such that $\vdash_S \neg(f_1 \wedge \ldots \wedge f_n)$. If in addition, for any sentence f, Γ contains one of f and $\neg f$ then Γ is *maximal consistent*. For arbitrary sets of sentences Γ_1 and Γ_2, we also define

$$\Gamma_1 * \Gamma_2 \quad = \quad \{(f; g) \mid f \in \Gamma_1,\ g \in \Gamma_2\}.$$

We denote by $\mathcal{L}^+$ a new ITL language obtained by adding to $\mathcal{L}$ an infinite set of *rigid* constants $B = \{b_0, b_1, \ldots\}$ not already in $\mathcal{L}$. A set Δ of sentences of $\mathcal{L}^+$ is said to have witnesses in B if for every sentence $(\exists x)f(x)$ of Δ, there is a b_j in B such that $f(b_j) \in \Delta$.

Assume Γ is a consistent set of sentences of $\mathcal{L}$. By a classic construction, it is possible to obtain a set $\Gamma^\star$

of sentences of $\mathcal{L}^+$ such that $\Gamma \subseteq \Gamma^\star$, $\Gamma^\star$ is maximal consistent and $\Gamma^\star$ has witnesses in B [4, 7].

Let Σ be the set of all rigid sentences of $\Gamma^\star$ and $\equiv$ be the equivalence relation on B defined by

$$b_i \equiv b_j \text{ iff } (b_i = b_j) \in \Sigma.$$

A model $\mathcal{M}$ based on Σ and $\equiv$ can be constructed which will satisfy Γ.

- The worlds are the maximal consistent sets Δ of $\mathcal{L}^+$ such that $\Sigma \subseteq \Delta$ and Δ has witnesses in B.
- The relation R is defined by: $R(\Delta_1, \Delta_2, \Delta)$ iff $\Delta_1 * \Delta_2 \subseteq \Delta$.
- The domain is the set of equivalence classes of $\equiv$.

The interpretation of a symbol s of $\mathcal{L}^+$ in a world Δ is defined as in [4] by the two following rules, where $[b]$ denotes the equivalence class of a constant b of B.

- If s is a function symbol of arity n then for any constant $b_{i_1}, \ldots, b_{i_n}$ and b_j of B, we have

  $$I(s, \Delta)([b_{i_1}], \ldots, [b_{i_n}]) = [b_j]$$

  if and only if the sentence $(s(b_{i_1}, \ldots, b_{i_n}) = b_j)$ is in the set Δ.

- If s is a proposition symbol, we have

  $$I(s, \Delta)([b_{i_1}], \ldots, [b_{i_n}])$$

  if and only if the sentence $s(b_{i_1}, \ldots, b_{i_n})$ is in Δ.

The fact that $\Sigma \subseteq \Delta$ ensures that the interpretation of rigid symbols is the same in all worlds, hence $\mathcal{M}$ is a model in the sense of definition 1. The presence of L1 also implies the following proposition.

Proposition 3 *$\mathcal{M}$ is an S-model.*

PROOF: We only check the first condition of definition 2; the other case is symmetrical. Assume $R(\Delta_1, \Delta_2, \Delta)$, $R(\Delta_1', \Delta_2', \Delta)$ and $I(\ell, \Delta_1) = I(\ell, \Delta_1')$. By construction of I and the axioms of identity, there is a constant b_i of B such that $(\ell = b_i) \in \Delta_1$ and $(\ell = b_i) \in \Delta_1'$. If $f \in \Delta_2$ then $(\ell = b_i; f)$ is in Δ. By axiom L1, this implies that $\neg(\ell = b_i; \neg f)$ is also in Δ and it follows that $(\neg f) \notin \Delta_2'$. Then $f \in \Delta_2'$ and $\Delta_2' \subseteq \Delta_2$. By symmetry we obtain $\Delta_2 = \Delta_2'$. $\square$

It remains to verify that $\mathcal{M}$ actually satisfies Γ. This is a consequence of the following theorem.

Theorem 4 *For any world Δ of $\mathcal{M}$ and any sentence f of $\mathcal{L}^+$, $\Delta \models f$ iff $f \in \Delta$.*

The proof is by induction on f; details can be found in [7]. The only difficulty is to show that, if a sentence $(f; g)$ is in a set Δ of W, there are two worlds Δ_1, and Δ_2 such that $f \in \Delta_1$, $g \in \Delta_2$, and $\Delta_1 * \Delta_2 \subseteq \Delta$. For this, we introduce the notations

$$\begin{aligned} \widehat{\Gamma} &= \{f_1 \wedge \ldots \wedge f_k \mid f_1 \in \Gamma, \ldots, f_k \in \Gamma\}, \\ \overline{\Gamma} &= \{g \mid \vdash_S (f \Rightarrow g) \text{ for some } f \in \widehat{\Gamma}\}, \end{aligned}$$

and the following lemma.

Lemma 5 *If Γ is maximal consistent and $\widehat{\Gamma}_1 * \widehat{\Gamma}_2 \subseteq \Gamma$ then there are two maximal consistent sets $\Gamma_1^\star$ and $\Gamma_2^\star$ such that: $\Gamma_1 \subseteq \Gamma_1^\star$, $\Gamma_2 \subseteq \Gamma_2^\star$, and $\Gamma_1^\star * \Gamma_2^\star \subseteq \Gamma$.*

PROOF: The idea is that $\Gamma_1^\star$ must contain all sentences $\neg f$ such that for some $g \in \Gamma_2^\star$, $\neg(f; g) \in \Gamma$, and symmetrically for $\Gamma_2^\star$. Axioms A1 and rules Mono and N are sufficient to show that the following construction gives two such sets [7].

Sets $\Gamma_1^{(n)}$ and $\Gamma_2^{(n)}$ ($n \in \mathbb{N}$) are defined recursively by $\Gamma_1^{(0)} = \overline{\Gamma}_1$, $\Gamma_2^{(0)} = \overline{\Gamma}_2$, and

- for n even,

  $$\begin{aligned} \Gamma_1^{(n+1)} &= \overline{\Gamma_1^{(n)} \cup \{\neg f \mid \neg(f; g) \in \Gamma, g \in \Gamma_2^{(n)}\}} \\ \Gamma_2^{(n+1)} &= \Gamma_2^{(n)}, \end{aligned}$$

- for n odd,

  $$\begin{aligned} \Gamma_1^{(n+1)} &= \Gamma_1^{(n)}, \\ \Gamma_2^{(n+1)} &= \overline{\Gamma_2^{(n)} \cup \{\neg g \mid \neg(f; g) \in \Gamma, f \in \Gamma_1^{(n)}\}}. \end{aligned}$$

It can be shown by induction that $\Gamma_1^{(n)} * \Gamma_2^{(n)} \subseteq \Gamma$ for any n. Let Γ_1^+ and Γ_2^+ be the unions of the sets $\Gamma_1^{(n)}$ and $\Gamma_2^{(n)}$, respectively. We still have $\Gamma_1^+ * \Gamma_2^+ \subseteq \Gamma$ and this implies that Γ_1^+ and Γ_2^+ are consistent. Γ_1^+ can then be extended to a maximal consistent set $\Gamma_1^\star$ and $\Gamma_2^\star$ can be taken to be any maximal consistent extension of $\Gamma_2^+ \cup \{\neg g \mid \neg(f; g) \in \Gamma, f \in \Gamma_1^\star\}$. $\square$

Now, if Δ is a world of $\mathcal{M}$ and $(f; g) \in \Delta$, there are two constants b_i and b_j such that $(f \wedge \ell = b_i; g \wedge \ell = b_j)$ is in Δ (by construction of $\mathcal{M}$). The lemma can be applied with $\Gamma = \Delta$, $\Gamma_1 = \{f, \ell = b_i\}$, and $\Gamma_2 = \{g, \ell = b_j\}$; this gives two sets $\Delta_1 = \Gamma_1^\star$ and $\Delta_2 = \Gamma_2^\star$ such that $f \in \Delta_1$, $g \in \Delta_2$ and $\Delta_1 * \Delta_2 \in \Delta$. The rigidity axiom R ensures that $\Sigma \subseteq \Delta_1$ and $\Sigma \subseteq \Delta_2$;

axioms B and L1 imply that Δ_1 and Δ_2 have witnesses in B: Δ_1 and Δ_2 are two worlds of $\mathcal{M}$ (see [7]).

We conclude by the following completeness theorem.

Theorem 6 *Any sentence valid in $\mathcal{C}$ is provable by S.*

PROOF: If f is not provable by S then the set $\Gamma = \{\neg f\}$ is consistent. Applying the model construction sketched above yields an S-model $\mathcal{M}$ which satisfies Γ, hence f is not valid in $\mathcal{C}$. $\Box$

4 Reasoning about time intervals

4.1 Interval models

The axiomatic system S is adequate for the class $\mathcal{C}$ of models. However, the notion of S-models does not capture all the properties one can expect of time intervals. Except for the property of unique decomposition, no particular assumption has been made on the structure of the set of worlds W or the accessibility relation R of S-models. Yet we are mainly interested in models where W can be interpreted as a set of intervals and R represents the operation of chopping an interval in two parts. Such models can be defined as follows.

Definition 7 *An S-model $\mathcal{M} = (W, R, D, I)$ is called an interval model if there is a set T, totally ordered by a relation $\leqslant$, such that*

- *W is the set of pairs (t, t') of elements of T such that $t \leqslant t'$ (we denote these pairs by $[t, t']$),*
- *for any $[t_1, t_1']$, $[t_2, t_2']$ and $[t, t']$ of W,*

$$R([t_1, t_1'], [t_2, t_2'], [t, t']) \text{ iff } t = t_1,\ t_1' = t_2,\ t_2' = t'.$$

Informally, T is the underlying representation of time (we always assume linear time) and $[t, t']$ is the interval of time which begins at t and ends at t'. The relation R corresponds to splitting intervals as expected and the satisfaction rule for chop formulas can be rewritten

$$v, [t, t'] \models (f; g) \text{ iff there is } u \in T, \begin{cases} v, [t, u] \models f \\ v, [u, t'] \models g \\ t \leqslant u \leqslant t'. \end{cases}$$

So, $(f; g)$ is satisfied by an interval $[t, t']$ if f is true in some initial sub-interval and g in the rest of $[t, t']$.

The traditional semantics of ITL or the duration calculus [11, 15] does not mention possible worlds or accessibility relations but is given directly in terms of intervals, usually with a fixed time representation ($T = \mathbb{R}^+$ or $T = \mathbb{N}$). We do not make such an assumption; T may be any linearly ordered set.

It is also customary to interpret the length of an interval $[t, t']$ as the quantity $(t' - t)$. This implies that – like the temporal representation – the domain of interval models is fixed *a priori*: usually $D = \mathbb{R}$ or $D = \mathbb{N}$. We adopt a more abstract point of view. The domain D is not defined explicitly but is described by a set of first order axioms. A particular choice for these axioms defines a class of domains D and a sub-class of intervals models.

Axiomatizations of D require the presence of a minimal set of rigid symbols in the language $\mathcal{L}$. These symbols are used for expressing real-time, quantitative aspects as relations between the length of different intervals. Addition and comparison are clearly fundamental operations and it is also desirable to speak of point intervals of the form $[t, t]$. We call *interval languages* the ITL-languages used for reasoning about time intervals. As a minimum, we require that such languages contain the rigid functional symbol $+$ and the rigid constant 0.

4.2 Axiomatizations

We can now extend the system S in order to deal with interval models. We first add the following axioms (taken from [11, 6]):

A2: $((f; g); h) \Leftrightarrow (f; (g; h))$

L2: $\ell = x + y \Leftrightarrow (\ell = x; \ell = y)$

L3: $f \Rightarrow (f; \ell = 0)$
$\quad\ \ f \Rightarrow (\ell = 0; f)$.

A2 is valid in interval models, i.e. chop is associative. L2 is the additivity of lengths: the sum of the length of $[t, t']$ and $[t', t'']$ is the length of $[t, t'']$. L3 says that an interval can always be split into itself and a point interval (of length 0). L2 also introduces a strong link between the underlying time representation T and the domain D; properties of D will induce properties of T.

Proof systems for various classes of interval models can then be obtained by adding first order axioms for D. Several choices are possible, a minimal one is the following:

D1: $(x + y) + z = x + (y + z)$
D2: $x + y = y + x$
D3: $x + 0 = x$
D4: $x + y = x + z \Rightarrow y = z$
D5: $x + y = 0 \Rightarrow x = 0 \wedge y = 0$
D6: $(\exists z)(x + z = y \vee y + z = x)$.

This is consistent with traditional semantics where durations are either positive reals or natural numbers [6, 11, 15]. These axioms also imply that the relation $\leqslant$ defined by the first order formula

$$x \leqslant y \Leftrightarrow (\exists z)(x + z = y)$$

is a total order and that 0 is its smallest element.

More generally, we can assume that properties of D are given by a first order theory $\mathcal{T}$ in a language $\mathcal{L}_0$ which contains at least the two symbols $+$ and 0. Then $\mathcal{L}_0$ can be expanded to an ITL-language $\mathcal{L}$: the symbols of $\mathcal{L}_0$ become rigid symbols in $\mathcal{L}$ and $\mathcal{L}$ contains at least the flexible constant ℓ. An ITL proof system $S_\mathcal{T}$ in the language $\mathcal{L}$ can be constructed as an extension of $\mathcal{T}$: the axioms and inference rules of $S_\mathcal{T}$ are those of S plus A2, L2, L3, and the first order axioms of $\mathcal{T}$.

We can then associate with the first order theory $\mathcal{T}$ a sub-class $\mathcal{C}_\mathcal{T}$ of interval models: an interval model $\mathcal{M}$ is in $\mathcal{C}_\mathcal{T}$ if all the axioms of $S_\mathcal{T}$ are valid in $\mathcal{M}$. Provided $\mathcal{T}$ is consistent and the formulas D1 to D6 are theorems of $\mathcal{T}$ the class $\mathcal{C}_\mathcal{T}$ is non-empty: $\mathcal{T}$ possesses a first order model D and an interval model $\mathcal{M}$ can be constructed where D is both the domain and the time representation ($T = D$). Hence in this case, $S_\mathcal{T}$ is consistent too.

Interesting classes of models can be defined by choosing $\mathcal{T}$ adequately. Due to the presence of axiom L2, assumptions about time can be indirectly specified as properties of the addition. For example, by taking $\mathcal{T}$ to be the theory defined by D1–D6 together with the axiom

$$x \neq 0 \Rightarrow (\exists y)(\exists z)(x = y + z \wedge y \neq 0 \wedge z \neq 0),$$

one obtains a class $S_\mathcal{T}$ of dense-timed interval models.

4.3 Completeness

Under the previous assumptions ($\mathcal{T}$ is consistent and D1–D6 are theorems of $\mathcal{T}$) the system $S_\mathcal{T}$ is sound for $\mathcal{C}_\mathcal{T}$ by construction. In this section, we show that $S_\mathcal{T}$ is also complete. As before, the principle is to construct, for any set of sentences Γ consistent with respect to $S_\mathcal{T}$, an interval model $\mathcal{M}$ where Γ is satisfied.

Since $S_\mathcal{T}$ extends S, we can apply the model construction of section 3.3. This gives an S-model $\mathcal{M}_0 = (W_0, R_0, D_0, I_0)$ of Γ. Every theorem of $S_\mathcal{T}$ is valid in $\mathcal{M}_0$ but $\mathcal{M}_0$ is not an interval model. The main step is then to derive from $\mathcal{M}_0$ an interval model $\mathcal{M}$ which still satisfies Γ.

By construction, worlds of $\mathcal{M}_0$ are sets of sentences which are maximal consistent with respect to $S_\mathcal{T}$. If Δ_1, Δ_2 and Δ are three such worlds, then $R(\Delta_1, \Delta_2, \Delta)$ holds whenever $\Delta_1 * \Delta_2 \subseteq \Delta$. We also know that there is a world Δ_0 of W_0 such that $\Gamma \subseteq \Delta_0$, and that Γ is satisfied in Δ_0.

In order to obtain the interval model $\mathcal{M}$, we have to define a totally ordered set T used as a time representation. A possible construction is to define T as the set of pairs (Δ_1, Δ_2) of worlds of $\mathcal{M}_0$ such that $\Delta_1 * \Delta_2 \subseteq \Delta_0$. A relation $\leqslant$ can then be defined on T by setting

$$(\Delta_1, \Delta_2) \leqslant (\Delta_1', \Delta_2')$$

whenever there are b_i and b_j in B such that

$$(\ell = b_i) \in \Delta_1 \quad \text{and} \quad (\ell = b_i + b_j) \in \Delta_1'.$$

The validity of D1–D6 in $\mathcal{M}_0$ implies that $\leqslant$ is a total order.

The following property is fundamental in the construction of $\mathcal{M}$.

Proposition 8 *Given two elements $u = (\Delta_1, \Delta_2)$ and $u' = (\Delta_1', \Delta_2')$ of T with $u \leqslant u'$, there is a unique world $\Delta_{[u,u']}$ of $\mathcal{M}_0$ such that*

$$\Delta_1 * \Delta_{[u,u']} \subseteq \Delta_1' \quad \text{and} \quad \Delta_{[u,u']} * \Delta_2' \subseteq \Delta_2.$$

PROOF: There are two constants b_i and b_j in B such that $(\ell = b_i) \in \Delta_1$ and $(\ell = b_i + b_j) \in \Delta_1'$. The idea is to show that the set of sentences given below is consistent:

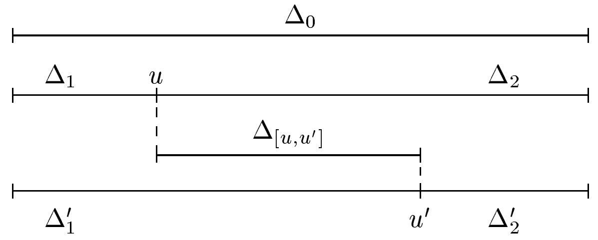
$$\begin{array}{rcl} A & = & \{\ell = b_j\} \\ & \cup & \{\neg g | \neg(f;g) \in \Delta_1', f \in \Delta_1\} \\ & \cup & \{\neg f | \neg(f;g) \in \Delta_2, g \in \Delta_2'\}. \end{array}$$

This follows from axioms L1–L2 and A1–A2 (see [7]).

Let $\Delta_{[u,u']}$ be a maximal consistent extension of A. Consider two sentences f of Δ_1 and g of $\Delta_{[u,u']}$. Assume $\neg(f;g)$ is in Δ_1' then $\neg g$ is in A by construction and this yields a contradiction. Hence we must have $(f;g) \in \Delta_1'$ and $\Delta_1 * \Delta_{[u,u']} \subseteq \Delta_1'$. Similarly, $\Delta_{[u,u']} * \Delta_2' \subseteq \Delta_2$.

Axioms R and B ensure that $\Delta_{[u,u']}$ is a world of $\mathcal{M}_0$. Uniqueness is due to the fact that $\mathcal{M}_0$ is an S-model. $\Box$

Informally, the situation can be depicted as follows:



The last proposition allows us to construct the interval model $\mathcal{M} = (W, R, D, I)$:

- W and R are obtained from the time representation T as indicated in definition 7.
- The domain D is equal to the domain D_0 of $\mathcal{M}_0$.
- The interpretation function I is defined by

$$I(s, [u, u']) = I_0(s, \Delta_{[u,u']}),$$

  for every symbol s in the language.

The definition of I implies that an atomic formula f is satisfied in the interval $[u, u']$ of $\mathcal{M}$ if and only if it is satisfied in the world $\Delta_{[u,u']}$ of $\mathcal{M}_0$. This property generalizes to arbitrary sentences.

Proposition 9 *Let $[u, u']$ be an interval of $\mathcal{M}$ and f a sentence of $\mathcal{L}^+$ then*

$$\mathcal{M}, [u, u'] \models f \quad \text{iff} \quad \mathcal{M}_0, \Delta_{[u,u']} \models f.$$

The proof is by induction on f and relies, for chop formulas, on the following lemmas [7].

Lemma 10 *Given three elements u, u', u'' of T such that $u \leqslant u' \leqslant u''$, $\Delta_{[u,u']} * \Delta_{[u',u'']} \subseteq \Delta_{[u,u'']}$.*

Lemma 11 *Let $[u, u'']$ be an interval of W and Δ_1 and Δ_2 be two worlds of $\mathcal{M}_0$ such that $\Delta_1 * \Delta_2 \subseteq \Delta_{[u,u'']}$ then there is an element u' of T such that*

$$u \leqslant u' \leqslant u'', \quad \Delta_{[u,u']} = \Delta_1, \quad \textit{and} \quad \Delta_{[u',u'']} = \Delta_2.$$

In order to check that Γ is satisfied in $\mathcal{M}$, it remains to find an interval $[u, u']$ in W such that $\Delta_{[u,u']} = \Delta_0$. Using axioms L3 and L1, it can be shown that there are two worlds Δ_1 and Δ_2 which contain the sentence $(\ell = 0)$ and such that

$$\Delta_1 * \Delta_0 \subseteq \Delta_0 \quad \text{and} \quad \Delta_0 * \Delta_2 \subseteq \Delta_0.$$

Then the two pairs $u = (\Delta_1, \Delta_0)$ and $u' = (\Delta_0, \Delta_2)$ belong to T and $\Delta_{[u,u']} = \Delta_0$.

This allows us to conclude by the completeness theorem for $S_{\mathcal{T}}$.

Theorem 12 *If a sentence f is valid in the class of interval models $\mathcal{C}_{\mathcal{T}}$ then f is provable by $S_{\mathcal{T}}$.*

PROOF: If f is not provable by $S_{\mathcal{T}}$ the set $\Gamma = \{\neg f\}$ is consistent with respect to $S_{\mathcal{T}}$. As indicated above, there is an S-model $\mathcal{M}_0$ of Γ in which all the axioms of $S_{\mathcal{T}}$ are valid. Let $\mathcal{M}$ be the interval model derived from $\mathcal{M}_0$. By proposition 9, the axioms of $S_{\mathcal{T}}$ are also valid in $\mathcal{M}$ and by the preceding remark, Γ is satisfied in $\mathcal{M}$. Hence f is not valid in $\mathcal{C}_{\mathcal{T}}$. $\square$

5 Conclusion

Complete axiomatic systems for different classes of ITL models can be obtained using the construction presented in this paper. The result is based on axiomatizations for interval models obtained as extensions of first order theories. Different proof systems are obtained by varying the first order axioms describing properties of D, the modal axioms being fixed. However, the main completeness result (theorem 12) immediately generalizes to other proof systems where new modal axioms are introduced. The result holds as long as A1–A2 and L1–L3 are theorems.

The technique is then quite general and we hope to extend it to the duration calculus [6, 11, 17]. This requires a new form of models involving a state represented as a collection of functions from T to a boolean domain and a generalization of the notion of duration of a state.

The results obtained do not guarantee completeness for *standard models* of ITL or the duration calculus. These models assume a particular time domain T and we do not know whether a complete first order theory $\mathcal{T}$ of T would extend to a complete ITL system $S_{\mathcal{T}}$ for standard models.

However, we can obtain complete proof systems for reasonably interesting classes, such as the general class of interval models or interval models in dense time. Also, complete and sound proof systems for a class of models relying on a notion of states as in [15] or [18] can be obtained easily [7]. This can confirm the practical interest of the various proof systems presented in the literature [6, 11, 15].

Another result can be derived by generalizing theorem 12. Many formalisms for reasoning about real-time systems adopt the assumption of finite variability: the state of a system cannot change infinitely often in a finite period of time. An important, though not surprising, result is that finite variability cannot be axiomatized in first order ITL. This is a consequence of a *compactness theorem* for ITL which is a simple extension of theorem 12 [7].

Acknowledgements

Many thanks to Anders Ravn who has provided precious comments and generated stimulating discussion about this work. The author also wishes to thank Martìn Abadi for his comments and Steve Schneider and Paul Mukherjee who agreed to read and correct preliminary versions of this paper.

References

[1] M. Abadi. The power of temporal proofs. *Theo-*

retical Computer Science, 65:35–83, 1989. Corrigendum in TCS 70 (1990), page 275.

[2] R. Alur, C. Courcoubetis, and D. Dill. Model-checking in dense real-time. *Information and Computation*, 104(1):2–34, May 1993.

[3] R. Alur and T. A. Henzinger. Real-time logics: Complexity and expressiveness. *Information and Computation*, 104(1):35–77, May 1993.

[4] C. C. Chang and H. J. Keisler. *Model Theory*. North-Holland, 1973.

[5] Z. Chaochen, M. R. Hansen, and P. Sestoft. Decidability and undecidability results for duration calculus. In *Proc. of STACS'93*, pages 58–68. Springer-Verlag, LNCS 665, 1993.

[6] Z. Chaochen, C. A. R. Hoare, and A. P. Ravn. A calculus of durations. *Information Processing Letters*, 40(5):269–276, December 1991.

[7] B. Dutertre. On First Order Interval Temporal Logic. Technical Report CSD-TR-94-3, Royal Holloway, University of London, January 1995.

[8] E. A. Emerson, A. Mok, A. P. Sistla, and J. Srinisavan. Quantitative temporal reasoning. In *Computer-Aided Verification*, pages 136–145. Springer-Verlag, LNCS 531, 1990.

[9] J. W. Garson. Quantification in modal logic. In *D. Gabbay and F. Guenthner (eds.), Handbook of Philosophical Logic*, volume II, pages 249–307. Reidel, 1984.

[10] J. Y. Halpern and Y. Shoham. A propositional modal logic of time intervals. *Journal of the ACM*, 38(4):935–962, October 1991.

[11] M. R. Hansen and Z. Chaochen. Semantics and completeness of duration calculus. In *Real-Time: Theory in Practice, REX Workshop*. Springer-Verlag, LNCS 600, 1992.

[12] T. A. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. Symbolic model checking for real-time systems. *Information and Computation*, 111(2):193–244, 1994.

[13] G. E. Hughes and M. J. Cresswell. *An Introduction to Modal Logic*. Routledge, 1990. First published by Methuen and Co., 1968.

[14] B. Moszkowski. Temporal logic for multilevel reasoning about hardware. *IEEE Computer*, 18(2):10–19, February 1985.

[15] B. Moszkowski. Some very compositional temporal properties. In *Programming Concepts, Methods, and Calculi*, pages 307–326. Elsevier Science B.V. (North-Holland), 1994.

[16] B. Paech. Gentzen-systems for propositional temporal logics. In *Proc. of the 2nd Workshop on Computer Science Logic*, pages 240–253. Springer-Verlag, LNCS 385, 1988.

[17] A. P. Ravn, H. Rischel, and K. M. Hansen. Specifying and verifying requirements of real-time systems. *IEEE Trans. on Software Engineering*, 19(1):41–55, January 1993.

[18] R. Rosner and A. Pnueli. A choppy logic. In *Proc. of the IEEE Symposium on Logic in Computer Science*, pages 306–313. IEEE, 1986.

[19] J. U. Skakkebæk and N. Shankar. Towards a duration calculus proof assistant in PVS. In *Formal Techniques in Real-time and Fault-Tolerant Systems*. Springer-Verlag, LNCS 863, September 1994.

[20] Y. Venema. A modal logic for chopping intervals. *Journal of Logic and Computation*, 1(4):453–476, 1991.